Research Article

International Journal of Distributed Sensor Networks

International Journal of Distributed Sensor Networks
2017, Vol. 13(8)

DOI: 10.1177/1550147717724308
journals.sagepub.com/home/ijdsn
SAGE

Security analysis and enhancements of an improved multi-factor biometric authentication scheme

YoHan Park[1], KiSung Park[2], KyungKeun Lee[3], Hwangjun Song[4] and YoungHo Park[2]

Abstract

Many remote user authentication schemes have been designed and developed to establish secure and authorized communication between a user and server over an insecure channel. By employing a secure remote user authentication scheme, a user and server can authenticate each other and utilize advanced services. In 2015, Cao and Ge demonstrated that An's scheme is also vulnerable to several attacks and does not provide user anonymity. They also proposed an improved multi-factor biometric authentication scheme. However, we review and cryptanalyze Cao and Ge's scheme and demonstrate that their scheme fails in correctness and providing user anonymity and is vulnerable to ID guessing attack and server masquerading attack. To overcome these drawbacks, we propose a security-improved authentication scheme that provides a dynamic ID mechanism and better security functionalities. Then, we show that our proposed scheme is secure against various attacks and prove the security of the proposed scheme using *BAN* Logic.

Keywords

Biometrics, authentication, cryptanalysis, mobile networks, anonymity

Date received: 24 August 2016; accepted: 9 July 2017

Academic Editor: Feng Hong

Introduction

With the rapid development of Internet technology and the smart device industry, users can access any service from anywhere.[1] In addition, the growth in network technology has made these services user-friendly and adoptable and mobile devices have become a vital part of our lives. Nowadays, people are able to easily utilize advanced services such as e-commerce, e-healthcare, and e-learning.[2]

Despite advantages of ubiquitous mobile computing technologies, several new threats have emerged. The transmission of data through insecure channels leads to the security challenges such as authentication, privacy, and integrity. And adversaries are considered to be sufficiently powerful to control communication over a public channel. To ensure authorized and secure communication, a user and server should verify their mutual legitimacy and exchange a session key, which can be used to transmit data securely.[3,4] Moreover, an anonymous authentication is required to provide secure communications between numerous network users while preserving privacy.

[1]Division of IT Convergence, Korea Nazarene University, Korea, Republic
[2]School of Electronics Engineering, Kyungpook National University, Daegu, Korea, Republic
[3]Mobile Division, Samsung Electronics, Korea, Republic
[4]Department of Computer Science and Engineering, Pohang University of Science and Technology (POSTECH), Korea, Republic

Corresponding author:
YoungHo Park, School of Electronics Engineering, Kyungpook National University, Daegu 702–701, Korea, Republic.
Email: parkyh@knu.ac.kr

To address security and authorized access in mobile environments, various remote user authentication schemes have been designed and developed. Remote user authentication is a common approach to verify the legitimacy of users who seek service and has become an indispensable component of service access. By employing a remote user authentication scheme, a server first authenticates remote users and grants service access only to those who are legitimate and authorized while rejecting unauthorized entities whose aim is to damage network security.

Smart card–based authentication schemes were introduced initially to resolve such security issues.[5–7] Recently, a large amount of research on password-based authentication schemes using smart cards has been presented.[3,8,9] However, password-based authentication schemes are vulnerable to identity/password guessing attacks and subject to inefficient password change policies. To resolve single-password authentication problems, several biometric-based remote user authentication schemes have been proposed.[2,10–12] In contrast to passwords, biometric information, such as irises, fingerprints, and palmprints, is considered to be a unique identifier of a user and is difficult to spoof. Therefore, biometric-based remote user authentication is inherently more secure and reliable than conventional authentication schemes.[13]

Li and Hwang[14] proposed an efficient biometric-based remote user authentication scheme in 2010. In 2011, Das[15] cryptanalyzed and improved Li and Hwang's[14] scheme. However, An[16] found out that Das'[15] scheme failed to provide mutual authentication and enhanced it to support secure authentication in 2012. In 2015, Cao and Ge[17] demonstrated that An's[16] scheme is vulnerable to replay attacks, in which an adversary can masquerade as the legal server. In addition, they mentioned that An's scheme does not provide user anonymity just as most recently presented biometric-based authentication schemes are not properly addressed, so An's scheme is insecure against user masquerading attack. Cao and Ge also proposed an improved multi-factor biometric authentication scheme to overcome the security weaknesses of An's scheme and support user anonymity. However, we point out their scheme fails to provide re-registration and does not withstand several attacks.

This article discusses the security vulnerability of Cao and Ge's scheme and proposes an enhanced multi-factor biometric authentication scheme with better security functionality than Cao and Ge's scheme. We provide an analysis of the security and efficiency of our proposed scheme. The major contributions of this study are summarized as follows:

Cryptanalysis of Cao and Ge's scheme. We cryptanalyze Cao and Ge's scheme and demonstrate the incorrectness of their scheme in re-registration phase and the vulnerability to the off-line ID guessing attack and server masquerading attack. We illustrate that an adversary can obtain the identity of any legal user of the system once he or she obtains the smart card of the user. Hence, the scheme does not provide user anonymity.

Enhancements of Cao and Ge's scheme. We propose an enhanced multi-factor biometric authentication scheme to overcome the security weaknesses of Cao and Ge's scheme. Our scheme supports the dynamic identity mechanism using timestamps and resists off-line ID guessing attack and server masquerading attack. We also provide password change phase to enhance the security of the system.

Security analysis against various attacks. We analyze the proposed scheme in security. Our scheme supports better security functionality than that of Cao and Ge's scheme. Our scheme is secure against off-line ID guessing attack, user masquerading attack, and server masquerading attack. In addition, it provides user anonymity, mutual authentication, session key agreement, efficient password change, and forward secrecy. We also prove that our scheme provides mutual authentication using Burrows–Abadi–Needham (*BAN*) Logic.[18]

Preliminaries

In this section, we present notations and then define Bio-Hashing.

Notations

The notations used throughout this article are described in Table 1.

Bio-hashing

Biometric technology often attracts attention in the area of unique user authentication in general authentication systems. Especially, the use of biometric information is extending steadily in cryptosystem for authentication purpose. However, imprint biometric characteristics (such as fingerprint, palmprint, retina, and iris) may not appear exactly the same in each scan. With high probability, imprinted biometric information rejects registered, legitimate users. To resolve the high false rejection rate, Jin et al.[19] proposed a two-factor authenticator on iterated inner products comprising a tokenized pseudo-random number and user-specific fingerprint features, which produces a set of user-specific compact codes; this is called Bio-Hashing. Later,

Table 1. Notations.

Notation	Meaning
C_i	User i
R_i	Trusted registration center i
S_i	Remote server i
ID_i	Actual identity of C_i
VID_i	Virtual identity of C_i
DID_i	Dynamic identity of C_i
PW_i	Password of C_i
B_i	Biometric template of C_i
SC_i	Smart card of user C_i
A_i	Adversary i
X_S	Secret key of S_i
x	Master key of R_i
K	Random number for registration of C_i
R_C	Random number generated by C_i
R_S	Random number generated by S_i
$\|\|$	Concatenate operation
$\oplus$	Bitwise XOR operation
$h()$	Secure hash function
$H()$	Bio-Hashing function
y_i	A unique number of C_i generated by the R_i
T_i	Timestamp

Lumini and Nanni[20] proposed an improvement of Bio-Hashing. As noted by Chang et al.,[21] Bio-Hashing is used to map a user's/patient's biometric feature onto user-specific random vectors to generate a code called a bio-code and then discretize the projection coefficients into zeroes and ones. Bio-Hashing is verified to be the most suitable and compatible technique that can be utilized in tiny smart devices such as smart cards and smart phones.[22]

Review of Cao and Ge's authentication scheme

In this section, we review Cao and Ge's authentication scheme. It comprises four phases: registration phase, re-registration phase, login phase, and authentication phase.

Registration phase

A user C_i first registers oneself at a trusted registration center R_i to obtain the service from the remote server S_i and receives a personalized smart card. A user chooses one's identity ID_i and password PW_i, imprints biometric information B_i, and then performs the following steps:

(R1) A user C_i chooses random number K and then compute $(PW_i \oplus K)$ and $(B_i \oplus K)$. Then, C_i submits $(ID_i, PW_i \oplus K, B_i \oplus K)$ to R_i via a secure channel.

(R2) R_i computes $f_i = h(B_i \oplus K), r_i = h(PW_i \oplus K) \oplus f_i, e_i = h(ID_i||X_S) \oplus r_i$.

(R3) R_i creates an entry in the account database for the user ID_i and store $n_i = 0$ in this entry. Then, R_i computes $EID_i = h(ID_i)||n_i$.

(R4) R_i computes $v_i = h(h(PW_i)||h(B_i)||X_S)$.

(R5) R_i sends a smart card that contains $\{EID_i, h(), f_i, e_i, n_i\}$ to C_i via a secure channel. Then, C_i stores a random K in the smart card.

Re-registration phase

(RR1) C_i chooses a new random number $K^{'}$ and then submits to R_i the identity ID_i, password information $(PW_i \oplus K^{'})$, and biometric information $(B_i \oplus K^{'})$ via a secure channel.

(RR2) R_i computes $v_i^{'} = h(h(PW_i)||h(B_i)||X_S)$ and compares it with v_i in the account database.

(RR3) If $v_i^{'}$ is equal to v_i, R_i sets $n_{i_{new}} = n_i + 1$. Then, R_i performs the following computations; $f_{i_{new}} = h(B_i \oplus K^{'}), r_{i_{new}} = h(PW_i \oplus K^{'}) \oplus f_{i_{new}}, e_{i_{new}} = h(ID_i||X_S) \oplus r_{i_{new}}$. And then EID_i is updated as $EID_i = h(ID_i)||n_{i_{new}}$.

(RR4) R_i sends a new smart card that contains the information $\{EID_i, h(), f_{i_{new}}, e_{i_{new}}, n_{i_{new}}\}$ to C_i via a secure channel. Then, C_i stores the random number $K^{'}$ in the smart card.

Login phase

In order to login to the remote server S_i, the user C_i performs the following steps using the smart card:

(L1) C_i imprints one's biometric information B_i, then the smart card SC_i computes $h(B_i \oplus K)$ and compares it with f_i. If it is valid, SC_i continues the following steps.

(L2) C_i chooses a random number R_C and inputs (ID_i, PW_i, R_C) into the smart card. Then, SC_i computes $r_i = h(PW_i \oplus K) \oplus f_i \oplus h(H(B_i), M_1 = e_i \oplus r_i, M_2 = M_1 \oplus R_C, M_3 = h(M_1||R_c)$.

(L3) SC_i computes $EID_i = h(ID_i)||n_i$.

(L4) C_i sends the login request message $\{EID_i, M_2, M_3\}$ to S_i.

Authentication phase

The user C_i and the remote server S_i verify the authenticity of each other in this phase as follows:

(A1) S_i checks the validity of the received EID_i by comparing $h(ID_i)||n_i$ in the account database.

(A2) If it is valid, S_i computes $M_4 = h(ID_i||X_S)$ and $M_5 = M_2 \oplus M_4$.

(A3) If $M_3 = h(M_4||M_5)$, S_i chooses a random number R_S and computes $M_6 = M4 \oplus R_S, M_7 = h(M_4||R_S)$.

(A4) Then, S_i sends the message $\{EID_i, M_6, M_7\}$ to C_i.

(A5) C_i computes $M_8 = M_6 \oplus M_1$ and checks whether $M_7 = h(M_1||M_8)$ or not. If it is valid, C_i computes $M_9 = h(M_1||R_C||M_8)$.

(A6) C_i sends the message $\{M_9\}$ to S_i.

(A7) S_i computes $M_{10} = h(M_4||M_5||R_S)$. If $M_{10} = M_9$, S_i accepts the user's login request and sends the message $\{M_{10}\}$ to C_i.

(A8) C_i checks whether $M_{10} = h(M_1||R_C||M_8)$ or not. If it is valid, C_i accepts S_i as the legitimate server.

Cryptanalysis of Cao and Ge's authentication scheme

In this section, we analyze the security problems of Cao and Ge's scheme. Cao and Ge[17] cryptanalyzed Younghwa An's[16] scheme and improved it to support better security functionality. However, we found out that Cao and Ge's remote user authentication scheme has security vulnerabilities. We assume that the capabilities of adversaries are as follows:[2,23]

- An adversary A_i has total control over the communication channel connecting the users and the remote server in login/authentication phase. Thus, the adversary can intercept, insert, delete, or modify any message transmitted via a public channel.
- An adversary may either steal a user's smart card or obtain a user's password, but not both.
- An adversary can extract the information stored in a smart card by means of analyzing the power consumption of the smart card.

Incorrectness in registration phase

Younghwa An[16] claimed that if the password PW_i and biometric information B_i of the user are revealed to the server, the insider in the server can obtain the user's password and biometric information directly. To protect the user's information from the insider in the server, Younghwa An concealed password and biometric information in registration phase using a XOR ($\oplus$) operation with user's information. Thus, the insider of the server may not know the user's password and biometric information. Cao and Ge referred to this method too; however, they failed to provide correctness. We show that registration phase of Cao and Ge's[17] scheme fails in correctness:

1. The user C_i submits $(ID_i, PW_i \oplus K, B_i \oplus K)$ to the server R_i via a secure channel.
2. R_i computes $v_i = h(h(PW_i)||h(B_i)||X_S)$.
3. From the received message $(ID_i, PW_i \oplus K, B_i \oplus K)$, R_i cannot extract PW_i and B_i. R_i cannot compute v_i too because it is computationally impossible to derive $h(PW_i)$ and $h(B_i)$.

We showed that Cao and Ge's scheme has fails in correctness and ultimately cannot proceed with re-registration phase because v_i is used to check the validity of the user in re-registration phase, but R_i cannot compute v_i. This means that it is vulnerable to user masquerading attack as is An's scheme. Therefore, the method of generation of v_i or the way to update user's identity must be revised.

Off-line identity guessing attack

The identity of a user is registered at the registration center. Users normally choose their social security ID, e-mail, phone number, and so on as their identity and are requested to input their identity, password, and biometric information in login phase. Although users attempt to keep their identities secret, identities are selected from a limited set that can be enumerated, and adversaries have sufficient power to guess from a limited set of identities in the off-line condition.[24] The complexity of this attack depends on the length of the identity. We show that Cao and Ge's scheme is vulnerable to off-line identity guessing attack.

1. An adversary A_i can know the information of the user C_i stored in a smart card. A_i extracts n_i from the smart card.
2. When C_i sends the login message to the remote server S_i, A_i records EID_i.
3. A_i selects a candidate identity $ID_i^{'}$, then computes $EID_i^{'} = h(ID_i^{'})||n_i$. A_i compares the computed $EID_i^{'}$ with the recorded EID_i. If they are equal, the adversary guesses the identity of the user C_i correctly. Otherwise, the adversary selects another candidate identity and repeats this step.

Once the identity of the user is revealed, an adversary can recognize and trace the user before the user performs re-registration phase. However, as we mentioned in "Incorrectness in registration phase," Cao and Ge's scheme fails in correctness to proceed re-registration phase. Therefore, the adversary can identify and trace the user continuously.

Server masquerading attack

Cao and Ge analyzed the security of their authentication scheme against server masquerading attack by sending M_{10}, because C_i will finally find that the

equation M_{10} is not equal to M_9. However, C_i cannot know whether the sender of the message $\{EID_i, M_6, M_7\}$ is valid or not. Thus, the message M_9, C_i sends to the server, can be sent to the adversary attempting to masquerade as the legal server. Finally, the adversary who sends the $\{EID_i, M_6, M_7\}$ can obtain the message M_9 and send a valid message M_{10} by replacing it with the message M_9 received right before the communication. We show that Cao and Ge's scheme is vulnerable to server masquerading attack:

1. An adversary A_i can intercept the message $\{EID_i, M_6, M_7\}$ over the communication channel.
2. When a new session is opened, A_i sends the replaying message $\{EID_i, M_6, M_7\}$ to C_i during the authentication phase pretending to the legal server.
3. C_i sends the message M_9 to the adversary because he or she still don't know whether the server is valid or not using the message $\{EID_i, M_6, M_7\}$.
4. A_i responds with the message M_{10} which is the received message M_9 from C_i.
5. C_i checks whether M_{10} is equal to M_9 or not. Because $M_9 = M_{10}$, C_i regards the adversary as the legal server.

An adversary can masquerade as the server before the user performs re-registration phase. However, as we mentioned in "Incorrectness in registration phase," Cao and Ge's scheme fails in correctness to proceed with re-registration phase. Therefore, the adversary can continue pretending to be the legal server.

The proposed remote user authentication scheme

We propose a dynamic ID-based multi-factor biometric authentication scheme to overcome the security problems of Cao and Ge's remote user authentication scheme. In the proposed scheme, we use timestamps to support the dynamic identity mechanism and resist off-line ID guessing attack. We assume that the registration center and the remote server are trustworthy and share a server's secret key X_S and a master key of the registration center x in advance. Our scheme comprises four phases: registration phase, login phase, authentication phase, and password change phase.

Registration phase

In this phase, a user C_i chooses one's identity ID_i and password PW_i, and imprints biometric information B_i, then performs following steps:

(R1) A user C_i chooses a random number K, and then computes $(PW_i \oplus K)$ and $(H(B_i) \oplus K)$. Then, C_i submits $(ID_i, PW_i \oplus K, H(B_i) \oplus K)$ to R_i via a secure channel.

(R2) R_i chooses an unique number y_i of C_i and computes $f_i = h(H(B_i) \oplus K), r_i = h(PW_i \oplus K) \oplus f_i$, $e_i = h(ID_i||X_S) \oplus r_i, VID_i = h(y_i||X_S) \oplus ID_i \oplus h(PW_i \oplus K||h(H(B_i) \oplus K)), Z_i = y_i \oplus h(x)$, and $G_i = h(h(ID_i|| X_S))$.

(R3) R_i creates an entry in the ID_i and virtual identity VID_i in this entry.

(R4) R_i stores $\{VID_i, h(), H(), f_i, e_i, Z_i, G_i\}$ into the smart card SC_i delivers it to C_i via a secure channel.

(R5) Upon receiving SC_i, C_i stores a random K in the smart card.

Figure 1 illustrates the registration phase of the proposed remote user authentication scheme.

Login phase

In order to login to the remote server S_i, the user C_i performs following steps using the smart card as follows:

(L1) C_i imprints one's biometric information B_i and computes $H(B_i)$, then SC_i computes $h(H(B_i) \oplus K)$ and compares it with f_i. If it is valid, SC_i continues the following steps.

(L2) C_i chooses a random number R_C and inputs (ID_i, PW_i, R_C) into the smart card. Then, SC_i computes $r_i^{'} = h(PW_i \oplus K) \oplus f_i, M_1 = e_i \oplus r_i^{'}, M_2 = M_1 \oplus R_C, M_3 = h(M_1||R_C||T_1)$. To generate dynamic identity DID_i, C_i computes $DID_i = VID_i \oplus h(h(y_i||X_S)||T_1)$, where $h(y_i||X_S) = VID_i \oplus ID_i \oplus h(PW_i \oplus K||h(H(B_i) \oplus K))$.

(L3) C_i sends the login request message $\{DID_i, Z_i, M_2, M_3, T_1\}$ to S_i.

Authentication phase

The user C_i and the remote server S_i verify the authenticity of each other and generate a session key in this phase as follows.

(A1) Upon receiving $\{DID_i, Z_i, M_2, M_3, T_1\}$, S_i verifies $T_1 - T \leq \Delta T$. If the verification is failed, S_i stops the session. Otherwise, S_i checks the validity of the received DID_i by comparing $VID_i^{'} = VID_i$ in the account database, where $VID_i^{'} = DID_i \oplus h(h(y_i||X_S)||T_1)$, $y_i = Z_i \oplus h(x)$.

(A2) If the verification is failed, S_i stops the session. Otherwise, S_i computes $M_4 =$

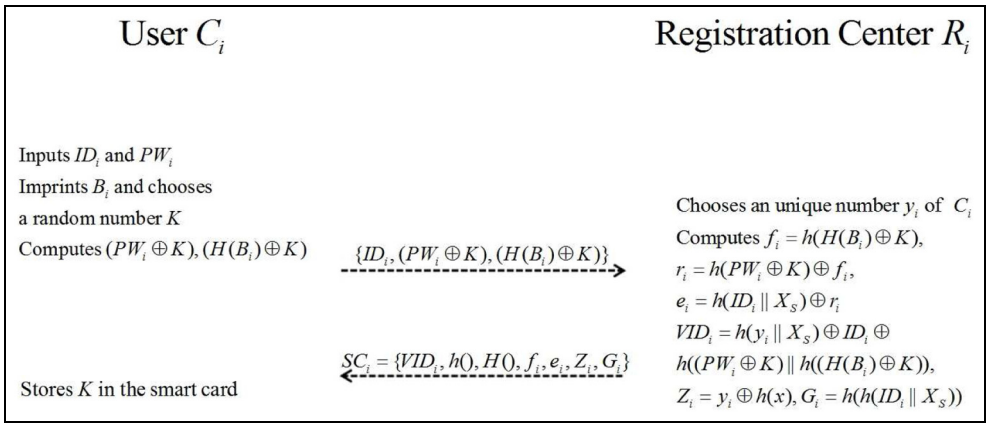

Figure 1. Registration phase.

$h(ID_i||X_S)$, $M_5 = M_2 \oplus M_4$ and checks whether $M_3 = h(M_4||M_5||T_1)$ or not.

(A3) If the verification is failed, S_i stops the session. Otherwise, S_i chooses a random number R_S and computes $M_6 = M_4 \oplus R_S$, $M_7 = h(M_4||R_S||T_2)$. And then, S_i sends the message $\{M_6, M_7, T_2\}$ to C_i.

(A4) C_i verifies $T_2 - T \leq \Delta T$. If the verification is failed, C_i stops the session. Otherwise, C_i computes $M_8 = M_1 \oplus M_6$, and then checks whether $M_7 = h(M_1||M_8||T_2)$.

(A5) If the verification is failed, C_i stops the session. Otherwise, C_i computes $M_9 = h(M_1||R_C||M_8||T_2)$ and sends the message $\{M_9, T_3\}$ to S_i. And then C_i computes a session key $SK = h(R_C||M_8||T_2||T_3||M_9)$.

(A6) S_i verifies $T_3 - T \leq \Delta T$. If the verification is failed, S_i stops the session. Otherwise, S_i checks whether $M_9 = h(M_4||M_5||R_S||T_2)$ or not. If the verification is failed, S_i stops the session. Otherwise, S_i computes a session key $SK' = h(M_5||R_S||T_2||T_3||M_9)$ and sends $h(SK')$ to C_i.

(A7) C_i checks the validity of $h(SK')$ by comparing $h(SK)$. If the verification succeeds, C_i authenticates S_i. On the success of authentication, C_i and S_i have a common session SK.

Figure 2 illustrates our proposed remote user authentication scheme.

Password change phase

The smart card establishes an authorized session with the user C_i to verify the correctness of input parameters (identity, password, and biometric information). C_i updates the password without interaction with the remote server or the registration center:

(P1) C_i inserts the smart card SC_i into the card reader. Then, C_i inputs ID_i, PW_i and a new password PW_i^{new}, and then imprints B_i.

(P2) SC_i computes $f_i' = h(H(B_i) \oplus K)$ and then verifies biometric information by comparing $f_i' = f_i$. If the verification is failed, the session is terminated. Otherwise, SC_i computes $r_i' = h(PW_i \oplus K) \oplus f_i'$, then checks the validity of ID_i and PW_i by comparing $G_i = h(h(e_i \oplus r_i'))$.

(P3) If the verification is failed, the session is terminated. Otherwise, SC_i computes $r_i^{new} = h(PW_i^{new} \oplus K) \oplus f_i', e_i^{new} = e_i \oplus r_i' \oplus r_i^{new}$. Then, SC_i stores e_i^{new} in place of e_i.

Figure 3 illustrates password change of the proposed remote user authentication scheme.

Analysis

In this section, we describe an analysis of our proposed authentication scheme with respect to security and performance. We assume that the capabilities of adversaries are the same as those from our cryptanalysis of Cao and Ge's authentication scheme. We first prove the security of our proposed scheme using *BAN* Logic.[18] Then, we show the security analysis of proposed scheme against various attacks.

Authentication proof based on BAN logic

In this section, we analyze the security of our proposed authentication scheme with *BAN* Logic[18] which is a formal analysis method for authentication protocols. Table 2 illustrates notations used in *BAN* Logic.

1. The *BAN* Logic postulates
   a. *Message meaning rule* concerns the interpretation of messages. They all derive beliefs about the origin of messages.

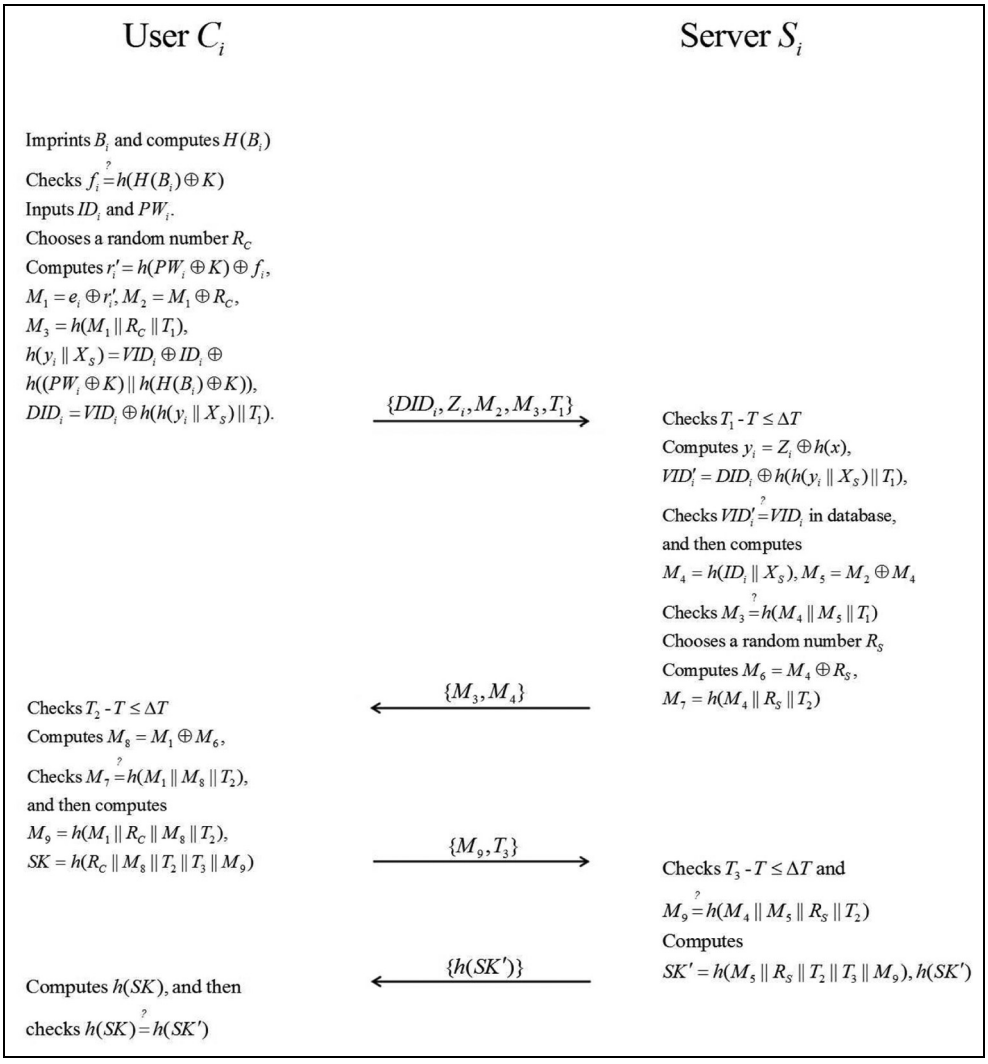

Figure 2. Proposed remote user authentication scheme.

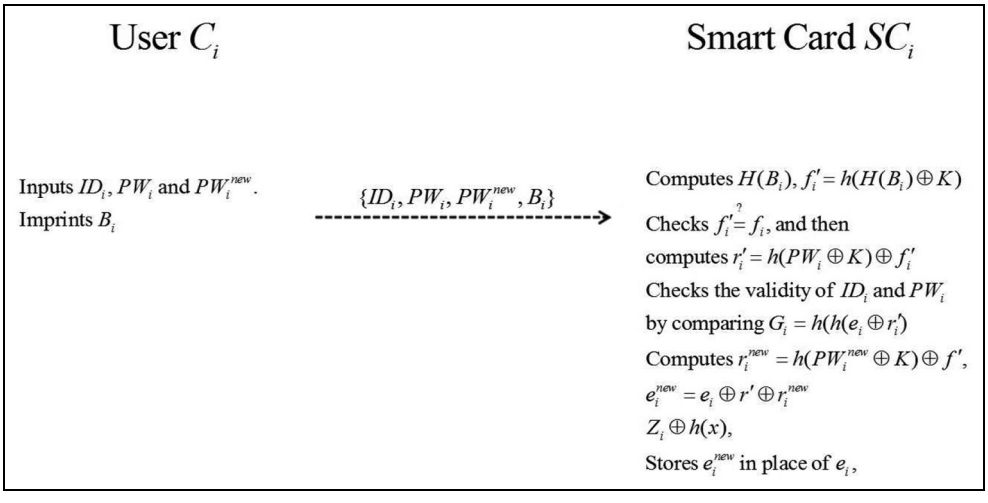

Figure 3. Password update phase.

Table 2. BAN logic notations.

Notations	Meaning
$P\|\equiv X$	P *believes* X
$P \triangleleft X$	P *sees* X
$P\|\sim X$	P *once said* X
$P \Rightarrow X$	P has *jurisdiction over* X
$\#(X)$	X is *fresh*
$P \overset{K}{\leftrightarrow} Q$	P and Q may use the *shared key* K
$P \overset{X}{=} Q$	X is a *secret* known only to P and to Q
$\langle X \rangle_Y$	X *combined with* the formula Y
$(X)_K$	X hashed under the key K
$\{X\}_K$	X encrypted under the key K

For shared keys, we postulate

$$\frac{P \text{ believes } Q \overset{K}{\leftrightarrow} P, P \text{ sees } \{X\}_K}{P \text{ believes } Q \text{ said } X}$$

That is, if P believes that the key K is shared with Q and sees X encrypted under K, then P believes that Q once said X.

b. *Nonce-verification rule* expresses the check that a message is recent, and hence, that the sender still believes in it

$$\frac{P \text{ believes fresh } (X),\ P \text{ believes } Q \text{ said } X}{P \text{ believes } Q \text{ believes } X}$$

That is, if P believes that X could have been uttered only recently and that Q once said X, then P believes that Q believes X.

c. *Jurisdiction rule* states that if P believes that Q has jurisdiction over X, then P trusts Q on the truth of X

$$\frac{P \text{ believes } Q \text{ controls } X,\ P \text{ believes } Q \text{ believes } X}{P \text{ believes } X}$$

d. If a principal sees a formula, then he also sees its components, provided he knows the necessary keys

$$\frac{P \text{ sees } (X, Y)}{P \text{ sees } X}, \quad \frac{P \text{sees } \langle X \rangle_Y}{P \text{ sees } X}$$

$$\frac{P \text{believes } Q \overset{K}{\leftrightarrow} P(,)P \text{ sees } [X]_K}{P \text{ sees } X}$$

$$\frac{P \text{ believes } \overset{K}{\mapsto} P,\ P \text{ sees } [X]_K}{P \text{ sees } X}$$

$$\frac{P \text{ believes } \overset{K}{\mapsto} P,\ P \text{ sees } [X]_{K^{-1}}}{P \text{ sees } X}$$

Note that if P sees X and P sees Y, it does NOT follow that P sees (X, Y) since that means that X and Y were uttered at the same time.

e. *Freshness-conjuncatenation rule* states that if one part of the formula is fresh, then the entire formula must be fresh

$$\frac{P \text{ believes fresh}(X)}{P \text{ believes fresh}(X, Y)}$$

2. *Security goals*. The proposed scheme will satisfy the following goals

$$g_1.\quad C_i|\equiv C_i \overset{SK}{\leftrightarrow} S_i$$

$$g_2.\quad S_i|\equiv C_i \overset{SK}{\leftrightarrow} S_i$$

$$g_3.\quad C_i|\equiv S_i|\equiv C_i \overset{SK}{\leftrightarrow} S_i$$

$$g_4.\quad S_i|\equiv C_i|\equiv C_i \overset{SK}{\leftrightarrow} S_i$$

3. *Idealized scheme*. We transform our scheme into the idealized form as follows

$$Msg_1.\quad C_i \rightarrow S_i : <VID_i>_{h(y_i||X_S)}, (R_C)_{h(ID_i||X_S)}, <Y_i>_{h(x)}$$

$$Msg_2.\quad S_i \rightarrow C_i : (R_S)_{h(ID_i||X_S)}$$

$$Msg_3.\quad C_i \rightarrow S_i : (R_C, R_S)_{h(ID_i||X_S)}$$

$$Msg_4.\quad S_i \rightarrow C_i : (R_C, R_S, C_i \overset{SK}{\leftrightarrow} S_i)_{h(ID_i||X_S)}$$

4. *Initiative premises*. We make the assumptions about the initial state of the scheme to analyze the proposed scheme as follows

$$p_1.\quad C_i|\equiv C_i \overset{h((y_i||X_S))}{\longleftrightarrow} S_i$$

$$p_2.\quad S_i|\equiv C_i \overset{h((y_i||X_S))}{\longleftrightarrow} S_i$$

$$p_3.\quad C_i|\equiv C_i \overset{h((ID_i||X_S))}{\longleftrightarrow} S_i$$

$$p_4.\quad S_i|\equiv C_i \overset{h((ID_i||X_S))}{\longleftrightarrow} S_i$$

$$p_5.\quad C_i|\equiv S_i|\equiv C_i \overset{h((ID_i||X_S))}{\longleftrightarrow} S_i$$

$$p_6.\quad S_i|\equiv C_i|\equiv C_i \overset{h((ID_i||X_S))}{\longleftrightarrow} S_i$$

$$p_7.\quad C_i|\equiv \#(R_S)$$

$$p_8.\quad S_i|\equiv \#(R_C)$$

$$p_9.\quad C_i|\equiv S_i \Rightarrow C_i \overset{SK}{\leftrightarrow} S_i$$

$$p_{10}.\quad S_i|\equiv C_i \Rightarrow C_i \overset{SK}{\leftrightarrow} S_i$$

$$p_{11}.\quad C_i|\equiv S_i \overset{h(x)}{\leftrightarrow} RC$$

5. Security analysis of the idealized form of the proposed scheme

a_1. According to Msg_1, We could get

$$S_i \triangleleft <VID_i>_{h(y_i||X_S)}, (R_C)_{h(ID_i||X_S)}, <y_i>_{h(x)}$$

a_2. According to p_2 and p_4, we apply the message-meaning rule to obtain

$$S_i|\equiv C_i|\sim <VID_i>_{h(y_i||X_S)}, (R_C)_{h(ID_i||X_S)}$$

a_3. According to p_8, we apply the freshness-conjuncatenation rule to obtain

$$S_i|\equiv \#(<VID_i>_{h(y_i||X_S)}, (R_C)_{h(ID_i||X_S)})$$

Then, we apply the nonce-verification rule to obtain

$$S_i|\equiv C_i|\equiv <VID_i>_{h(y_i||X_S)}, (R_C)_{h(ID_i||X_S)}$$

a_4. According to Msg_3, we could get

$$S_i \triangleleft (R_C, R_S)_{h(ID_i||X_S)}$$

a_5. According to p_4, we apply the message-meaning rule to obtain

$$S_i|\equiv C_i|\sim (R_C, R_S)_{h(ID_i||X_S)}$$

a_6. According to p_8, we apply the freshness-conjuncatenation rule to obtain

$$S_i|\equiv \#(R_C, R_S)_{h(ID_i||X_S)}$$

Then, we apply the nonce-verification rule to obtain

$$S_i|\equiv C_i|\equiv (R_C, R_S)_{h(ID_i||X_S)}$$

a_7. According to a_6 and p_6 and $SK = h(R_C, R_S, h(ID_i||X_S))$, we could obtain

$$S_i|\equiv C_i|\equiv C_i \overset{SK}{\leftrightarrow} S_i \quad \text{(Goals 4)}$$

a_8. According to a_7 and p_9, we apply the jurisdiction rule to obtain

$$S_i|\equiv C_i \overset{SK}{\leftrightarrow} S_i \quad \text{(Goals 2)}$$

a_9. According to Msg_4, we could get

$$C_i \triangleleft (R_C, R_S, C_i \overset{SK}{\leftrightarrow} S_i)_{h(ID_i||X_S)}$$

a_{10}. According to p_3, we apply the message-meaning rule to obtain

$$C_i|\equiv S_i|\sim (R_C, R_S, C_i \overset{SK}{\leftrightarrow} S_i)_{h(ID_i||X_S)}$$

a_{11}. According to p_7, we apply the freshness-conjuncatenation rule to obtain

$$C_i|\equiv \#(R_C, R_S, C_i \overset{SK}{\leftrightarrow} S_i)_{h(ID_i||X_S)}$$

Then, we apply the nonce-verification rule to obtain

$$C_i|\equiv S_i|\equiv (R_C, R_S, C_i \overset{SK}{\leftrightarrow} S_i)_{h(ID_i||X_S)}$$

a_{12}. According to a_{11}, we apply the *BAN* Logic rule to break conjunctions to produce

$$C_i|\equiv S_i|\equiv C_i \overset{SK}{\leftrightarrow} S_i \quad \text{(Goals 3)}$$

a_{13}. According to a_{12} and p_9, we apply the jurisdiction rule to produce

$$C_i|\equiv C_i \overset{SK}{\leftrightarrow} S_i \quad \text{(Goals1)}$$

According to (Goal 1), (Goal 2), (Goal 3), and (Goal 4), we know that C_i and S_i believe SK is shared.

Security analysis against various attacks

Off-line ID guessing attack. The smart card and login message contain pseudo identities, VID_i and DID_i, which are random values. Suppose an adversary A_i obtains these values and the smart card SC_i. To derive an actual identity ID_i from VID_i, the adversary is required to

guess both $h(y_i||X_S)$ and ID_i concurrently. The probability of guessing them correctly, when ID_i is composed of n characters and the hash value is taken as 160 bits, is approximately $1/2^{6n+160}$ and it is considered to be a computationally infeasible problem.[21,25] The complexity of our proposed scheme against this attack is higher than that of Cao and Ge's scheme. To derive ID_i from DID_i, A_i is required to compute more, which means that the complexity is higher, because DID_i is dynamic.

User masquerading attack. A_i is required to compute a valid login request to impersonate a legal user. A_i may attempt to login to S_i using the message $\{DID_i, Z_i, M_2, M_3, T_1\}$. However, DID_i is dynamic in every session, so A_i cannot use the message repeatedly. Moreover, A_i cannot generate a valid dynamic identity either because he or she cannot know $h(y_i||X_S)$.

Server masquerading attack. To masquerade as a legal server, A_i must compute messages $\{M_6, M_7\}$ and $h(SK)$. An's[16] scheme and Cao and Ge's[17] scheme were vulnerable to this attack because A_i could replay messages captured in a previous session. However, our proposed scheme is secure against this attack because we use timestamps, and the messages are fresh in each session.

User anonymity. We use pseudo identities to hide an actual identity. To derive ID_i from VID_i or DID_i, A_i should know $h(y_i||X_S)$; however, it is computationally infeasible to correctly guess y_i and X_S concurrently. Therefore, it is difficult for A_i to derive ID_i from pseudo identities.

Mutual authentication. The server verifies the legitimate user by checking the equivalence $M_9 = h(M_4||M_5||R_S||T_2)$. Likewise, the user ensures the validity of the server by checking the equivalence $h(SK^{'}) = h(SK)$. However, A_i can masquerade as neither the legitimate user nor the server. Therefore, the proposed scheme provides proper mutual authentication.

Forward secrecy. Suppose that the server's secret key X_S is compromised, the identity ID_i is still unknown to A_i. Therefore, $h(ID_i||X_S)$ is kept secret and R_C and R_S remain secure. Thus, compromise of X_S does not allow A_i to compute the previous session keys.

We compare the functionality features and the computational cost of the proposed scheme with those of other existing schemes. Table 3 compares the functionality features provided by our scheme with those of other existing schemes. ○ denotes the scheme provides the property; × denotes the scheme does not provide the property; NA denotes the scheme does not consider the property.

Performance

In Table 4, we compare the computational cost. T_h denotes the computation time for hash function; T_H denotes the computation time for Bio-Hashing

Table 3. Comparisons of the functionality features.

	Das's scheme[15]	Younghwa An's scheme[16]	Cao and Ge's scheme[17]	Proposed scheme
Resists ID guessing attack	NA	NA	×	○
Resists user masquerading attack	×	×	○	○
Resists server masquerading attack and replay attack	×	×	×	○
Provides user anonymity	×	×	×	○
Provides mutual authentication	×	×	×	○
Provides session key agreement	×	×	×	○
Provides efficient password change	×	×	×	○
Provides forward secrecy	NA	NA	NA	○

Table 4. Comparisons of the computation costs.

	Das's scheme[15]			Younghwa An's scheme[16]			Cao and Ge's scheme[17]			Proposed scheme		
	User	RC	Server	User	RC	Server	User	RC	Server	User	RC	Server
Registration	0	$3T_h$	0	0	$3T_h$	0	0	$7T_h$	0	T_H	$6T_h$	0
Login	$2T_h$	0	0	$3T_h$	0	0	$4T_h$	0	0	$1T_H + 5T_h$	0	0
Authentication	$3T_h$	$3T_h$	$5T_h$	$2T_h$	0	$4T_h$	$3T_h$	0	$4T_h$	$4T_h$	0	$8T_h$
Total	$5T_h$	$3T_h$	$5T_h$	$5T_h$	$3T_h$	$4T_h$	$7T_h$	$7T_h$	$4T_h$	$2T_H + 9T_h$	$6T_h$	$8T_h$

function. XOR operations are not considered because it can be ignored comparing with T_h. Our scheme is constructed on one-way hash functions and XOR operations. The computation cost of ours is similar to An[16] and Cao and Ge,[17] but the proposed scheme provides the enhanced security functionalities and is secure against various attacks.

Conclusion

Users are able to access and utilize advanced services owing to the growth of Internet technology and smart devices. However, given the unsolved security problems and adversaries that are sufficiently powerful to control communication, users are exposed to malicious attacks, and extension of Internet service is limited. To ensure authorized and secure communication, a user and server should verify each other's legitimacy.

In this article, we demonstrated the security vulnerability of Cao and Ge's scheme and its incorrectness in re-registration phase. We noted that their scheme is vulnerable to off-line ID guessing attack and server masquerading attack and fails in correctness. In addition, we proposed an enhanced multi-factor biometric authentication scheme with better security functionality than that of Cao and Ge. Our scheme supports a dynamic identity mechanism using timestamps and resists off-line ID guessing attack and server masquerading attack. Our scheme satisfies all desirable security attributes, as demonstrated in the security analysis.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and Future Planning (2017R1A2B1002147).

References

1. Madhusudhan R and Mittal R. Dynamic id-based remote user password authentication schemes using smart cards: a review. *J Netw Comput Appl* 2012; 35(4): 1235–1248.
2. Mishra D, Kumari S, Khan MK, et al. An anonymous biometric-based remote user-authenticated key agreement scheme for multimedia systems. *Int J Commun Syst* 2017; 30: e2946.
3. Mishra D, Das AK, Chaturvedi A, et al. A secure password-based authentication and key agreement scheme using smart cards. *J Inform Secur Appl* 2015; 23: 28–43.
4. Lee CC, Li LH and Hwang MS. A remote user authentication scheme using hash functions. *ACM SIGOPS Oper Syst Rev* 2002; 36(4): 23–29.
5. Hwang MS and Li LH. A new remote user authentication scheme using smart cards. *IEEE T Consum Electr* 2000; 46(1): 28–30.
6. Sun HM. An efficient remote use authentication scheme using smart cards. *IEEE T Consum Electr* 2000; 46(4): 958–961.
7. Chien HY, Jan JK and Tseng YM. An efficient and practical solution to remote authentication: smart card. *Comput Secur* 2002; 21(4): 372–375.
8. Mishra D. On the security flaws in id-based password authentication schemes for telecare medical information systems. *J Med Syst* 2015; 39(1): 1–16.
9. Li X, Niu J, Liao J, et al. Cryptanalysis of a dynamic identity-based remote user authentication scheme with verifiable password update. *Int J Commun Syst* 2015; 28(2): 374–382.
10. Ku W, Chang S and Chiang M. Further cryptanalysis of fingerprint-based remote user authentication scheme using smartcards. *Electron Lett* 2005; 41(5): 240–241.
11. Chang CC, Chang SC and Lai YW. An improved biometrics-based user authentication scheme without concurrency system. *Int J Intell Inform Process* 2010; 1(1): 41–49.
12. Tan Z. A user anonymity preserving three-factor authentication scheme for telecare medicine information systems. *J Med Syst* 2014; 38(3): 1–9.
13. Li X, Niu J, Khan MK, et al. Robust three-factor remote user authentication scheme with key agreement for multimedia systems. *Secur Commun Netw* 2016; 9: 1916–1927.
14. Li CT and Hwang MS. An efficient biometrics-based remote user authentication scheme using smart cards. *J Netw Comput Appl* 2010; 33(1): 1–5.
15. Das AK. Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards. *IET Inform Secur* 2011; 5(3): 145–151.
16. An Y. Security analysis and enhancements of an effective biometric-based remote user authentication scheme using smart cards. *BioMed Res Int* 2012; 2012: 519723.
17. Cao L and Ge W. Analysis and improvement of a multifactor biometric authentication scheme. *Secur Commun Netw* 2015; 8(4): 617–625.
18. Burrows M, Abadi M and Needham RM. A logic of authentication. *P Roy Soc Lond A Mat* 1989; 426: 233–271.
19. Jin ATB, Ling DNC and Goh A. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recogn* 2004; 37(11): 2245–2255.
20. Lumini A and Nanni L. An improved biohashing for human authentication. *Pattern Recogn* 2007; 40(3): 1057–1065.
21. Chang YF, Yu SH and Shiao DRS. A uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care. *J Med Syst* 2013; 37(2): 1–10.
22. Belguechi R, Rosenberger C and Ait-Aoudia S. Biohashing for securing minutiae template. In: *Proceedings of the*

2010 20th international conference on pattern recognition (ICPR), Istanbul, Turkey, 23–26 August 2010, pp.1168–1171. New York: IEEE.

23. Kumari S, Khan MK and Li X. An improved remote user authentication scheme with key agreement. *Comput Electr Eng* 2014; 40(6): 1997–2012.
24. Cao T and Zhai J. Improved dynamic ID-based authentication scheme for telecare medical information systems. *J Med Syst* 2013; 37(2): 1–7.
25. Das AK and Goswami A. A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care. *J Med Syst* 2013; 37(3): 1–16.